

# Storage Networking Times

## Issue 9

October  
2008

### Inside this issue:

**Virtualisation:  
The Driver Behind  
the Next Phase of  
Consolidation** 3

**Storage Security  
Standards  
What Are They and  
What Do They Mean to  
Storage Consumers?** 5

**Regional Committee  
Update: France** 9

**Industry Events 2008-9** 10

## Letter From the Chair

Juergen Arnold, Chair, SNIA Europe, [eurochair@snia.org](mailto:eurochair@snia.org)



Welcome to SNW Europe 2008! I hope that like me you are looking forward to three days packed with SNIA tutorials, end user case studies, vendor presentations, product demos and much more.

For those of you looking for a more hands-on approach, look no further than the 'Hands-on lab' and the other activities offered by our training partners present at the conference. You will even be able to attend the classes to prepare for the SNIA accreditation exam, which can be taken at one of the many authorised centres across EMEA.

This year the organisers have once again put together a unique agenda, featuring speakers from the police force, football clubs, and hospitals to name but a few. Analysts will be sharing their forecasts for the upcoming months in the data storage industry and representatives from several SNIA forums and groups will be unveiling the latest developments around technologies and architectures.

And of course there will be plenty of opportunities to network and relax with your colleagues, peers and suppliers at the welcome reception on Monday evening, the happy hour after the last session on Tuesday and the Living XXL party on Tuesday night (don't forget to request your ticket from one of the party sponsors).

*(Continued on page 2)*

## Spotlight On: Storage Management Initiative

Frank Bunn, Chair, Storage Management Initiative, [SMI-europe-chair@snia.org](mailto:SMI-europe-chair@snia.org)



### On the Way to Becoming the Comprehensive Storage Management Standard

Recently, you might have had the impression that the storage market and with it the SNIA was increasingly focused on ILM, long-term archiving and XAM. However, behind the scenes, the SNIA has been working hard at further developing the storage management standard SMI-S.

What are the characteristics of a good standard and why does it often take longer to develop than was originally planned?

Alongside vendor independence and democratic operational leadership during the development process, the completeness of the standard, including possibilities for further development, detailed documentation, continuous complexity reduction and conformance testing are aspects that need to be taken into account at every stage.

**Vendor independence and democratic operational leadership (SMI-S Governance)**  
SMI-S is developed in the SNIA Technical Working Groups, which are open to all members. The SNIA defines policies for the working groups and a steering committee monitors the

*(Continued on page 2)*

## Letter From the Chair

*(Continued from page 1)*

In addition to SNW Europe, we run a series of one-day events across EMEA under the banner SNIA Europe Academy, which over 2,200 delegates have already attended. In the coming months we will visit Zurich, Dubai, Paris, Stockholm, Copenhagen and London. Visit [www.storage-academy.com](http://www.storage-academy.com) for dates and further information.

And don't forget that whether in person at one of our events or via our website you can always get in touch with SNIA Europe to provide feedback, request advice or share your experience of data storage!

I look forward to seeing you at the conference.

---

## Spotlight On: Storage Management Initiative

*(Continued from page 1)*

work and the co-operation among the various groups. The specifications that are developed are then made public to all vendors as standards via the ANSI (US) and the ISO (International).

### Completeness and Extensibility

The first SMI-S versions concentrated on basic functionality, such as discovery and easy administration of SAN systems. Later versions include new functionality such as thin provisioning, support for other systems like NAS or tape libraries, and optimisation of the standards in terms of their practical usage. SMI-S offers a platform for innovation. Vendor-specific extensions that leverage the defined format of the SMI-S can thus be easily integrated. SMI-S version 1.4.0 describes for the first time policies to make the vendors' own extensions compatible with the existing SMI-S profiles.

### Detailed Documentation

No developer really likes this point, but detailed documentation is necessary for a project to succeed. SMI-S 1.1 version contained 1,474 pages of documentation. In order to make the technical review process clearer, the content of the following version 1.2 was divided into 9 separate books. Professional editors increasingly help the SNIA to deal with complex documentation tasks.

### Reducing Complexity

Rather than re-invent the wheel, SMI-S makes use of existing standards developed by other industry groups. For example, the SMI-S 1.2 architecture book references 39 standards from T10 (SCSI), T11 (FC), T10 (ATA), IETF (iSCSI, Networking, Security), DMTF (Management) among other organisations. Current developments are increasingly focused on production readiness and the practical use of the standards in a developer's day-to-day work.

### Conformance Tests

Conformance testing was introduced as early as version 1.0. This enables vendors to prove that their hardware and software solutions conform with the relevant SMI-S profiles. In the course of the years, the testing process was continually expanded and improved. Over 500 SMI-S providers (including disk arrays and SAN switches) and SMI-S clients (SAN management applications) were tested via the SMI-S conformance tests. That proves that the programme is accepted and that the vendors expect a positive image and a competitive advantage in the market space as a result. The list of SMI-S certified products can be accessed on [http://www.snia.org/forums/smi/tech\\_programs/ctp/](http://www.snia.org/forums/smi/tech_programs/ctp/)

The characteristics described here make it obvious that the definition and development of a standard in such a wide area as storage management is not a simple task. The SNIA has set many important milestones and defined an interesting roadmap while the vendors are integrating the SMI-S specifications into their products.

SMI-S version 1.1.1 is currently in the middle of the standardisation process at ANSI and ISO. The work on SMI-S 1.2 was finished in Spring 2008 and released as a SNIA architecture. The new functions for SMI-S 1.3 were defined in IP storage environments for example and was released along with the Conformance Testing Program suite on 13 October 2008. Alongside describing policies for extending vendor-specific functions, SMI-S 1.4 will contain the integration with management frameworks as described in the last SMI-S update.

## Analyst Briefing: Virtualisation The Driver Behind the Next Phase of Consolidation

Hamish Macarthur, CEO and co-founder, Macarthur Stroud International [www.macarthurstroud.com](http://www.macarthurstroud.com)



We are living in changing times. Not only are there movements in the financial markets, but there are also changes afoot in the computing infrastructure. The key driver to these infrastructure changes is the need to reduce the cost of managing and operating systems, bringing cost targets in line with the business.

Information management must contribute to the profitability of the business. Supported by an adaptable system infrastructure to scale and flex with business priorities, computing services must be continuously available, robust and secure so that no data is lost and service levels are assured at all times.

The first phase of system consolidation was supported by the introduction of storage networking in the mid-nineties. The number of servers was reduced, while storage arrays were rationalised to deliver better utilisation. Significant return on investment was achieved in the process.

However, there are still further gains to be realised and virtualisation is enabling this. It delivers greater levels of consolidation through better utilisation of servers and storage. This helps to simplify management of the servers and storage platforms, contributing to a reduction in operational costs and capital expenditure.

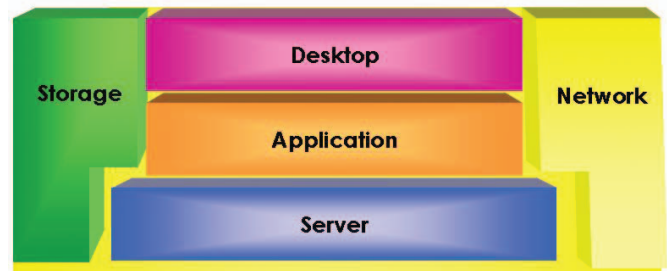
Further consolidation with the implementation of virtualisation leads to a reduction in the number of servers, storage arrays and other system devices. This in turn means that a smaller footprint is required, reducing estate costs. Equally important in today's world of high and increasing energy prices is the resultant reduction in power and cooling costs. And everyone in the IT department can make their contribution to the environmental policies of their organisations.

### Where Virtualisation Resides

Virtualisation resides in five levels of the system architecture:

- Desktop
- Application
- Server
- Storage
- Network.

### 5 Levels of Virtualisation



Implementing virtualisation is a journey. It is important to realise that the consolidation and management issues will be achieved step by step; at every stage the resources will be better utilised, the service levels will be maintained and costs will be contained or reduced.

In this article, we are concentrating on storage virtualisation. The initial view of storage virtualisation is the ability to establish a single pool of storage. But there are several facets to storage virtualisation, from allocating and provisioning through to security, data protection and archiving.

### Storage Virtualisation

Storage virtualisation supports the next wave of consolidation, new levels of data protection, migration of data to lower cost storage, a reduction in volume of stored data and a significant contribution to 'green' credentials.

Building on the concept of a single pool of storage, the other areas of storage virtualisation all contribute to better management of resources and continuous business operations.

**Dynamic Thin Provisioning of Virtualised Storage** - thin provisioning allows the implementation of the minimum amount of physical storage, yet creates the illusion to the application that it has enough or limitless storage available. As the demand for capacity grows, the virtualised allocation of storage can automatically grow to the maximum threshold capacity requested by the application. Once the appropriate rules, threshold and permissions have been set up, subsequent management tasks are considerably simplified.

**Delivering continuous data availability** - virtualisation has enabled new techniques and technology practices to be deployed that will move most businesses to a continuous

(Continued on page 4)

**Analyst Briefing: Virtualisation***(Continued from page 3)*

data protection model, enabling users to rewind their systems or recover information with the minimum risk of data loss. Examples of how this is delivered include:

- RAID provides automatic rebuilding of data in the case of one or two disks failing
- Point-in-time copies or *snapshots* take a copy of data that has changed
- Virtual Tape Libraries (VTLs) enable disk-to-disk (D2D) back-up, reducing back-up times and allowing for faster restore times
- Data replication processes will form the basis of new continuous system operations.

With virtualised servers, one issue to consider is how to replicate or move a system and the data to then run it on a new or different system platform. This process can also enable critical system management functions such as:

- Upgrading systems to new servers and disk arrays
- Internal system testing, ensuring that new software versions and patches can be fully tested before they are deployed in the production environment
- Moving the complete image of a system without having to worry if this is being moved to, or being moved from, a physical or a virtual environment.

**System imaging technologies**—application and data images to be taken and migrated to another system. Recovery times need to be rapid and the recovery process needs to be complete so that users experience minimum disruption. An automated process will be more timely to complete than a manual process subject to human error. Examples of how these technologies can be applied include:

- Application and system images being restored to the same or different servers
- Applications can migrate easily between physical and virtual systems
- Systems can be recovered or rebuilt on 'bare metal'
- Images can be recovered from different types of storage, including direct attach disk, NAS, SAN and tape
- Applications can be migrated to fewer servers overnight, powering down the unused servers and saving in energy costs.

**Reducing volumes of duplicated data**—de-duplication addresses the need to reduce the volumes of duplicate data that are stored. De-duplication identifies the same files, and sets up a process to keep one copy and provide a tag in all

other occurrences of this data directing the system to the master image. In the case of in-band (as opposed to post-process) data deduplication, this results in less disk space required to store the data, faster back-ups and lower number of duplicated copies of data.

**Virtual Tape Libraries (VTLs)**—Virtual Tape Libraries write data to disk as if it were writing to tape, with the primary benefits being speed and the completion of back-up within normal working hours. Initial and multiple back-up copies can be held on the VTL for fast recovery. Virtual tape functions are aligned with off-loading the data to tape. Tape becomes a secondary back-up to enable copies to be moved offsite or archived for longer periods. By introducing VTL into the back-up process, back-up windows are dramatically reduced.

**Data management costs versus physical hardware**—managing the data resident on the disks and tapes costs up to five times the cost of the hardware. Management is necessary to allocate resources, to complete data protection practices such as backup and recovery, track and report activities and, where possible, categorise data for long-term storage, regulatory or disposal purposes. Virtualisation builds on these foundations and enables CIOs to address the issue of data management before it becomes a major business problem.

**Data migration and tiered storage** - moving and migrating data to the most appropriate locations is a fundamental element of effective data management. This arises for cost and system management reasons. Examples for data migration include:

- Moving data that has not been accessed for a long time to a lower cost storage device
- System testing, where new application software can be tested with real data sets before it is deployed in the production environment
- Data protection and additional system images that can be maintained on lower cost SATA, MAID or tape solutions.

**File systems and storage architecture**—Establishing a single file system, with a global namespace, enables the system to scale and grow without users noticing the physical changes. Attention can be focused on providing a service to users, whether they are supported by one system at one location or supported by physically separate disk arrays or file servers. Data protection, data security and de-duplication can be implemented consistently across the system architecture with centralised management policies.

*(Continued on page 5)*

**Analyst Briefing: Virtualisation***(Continued from page 4)***Using Virtualisation to Improve Return on Investment**

Businesses are demanding a better return from their investments in IT.

As a result virtualisation technologies are being implemented across all layers of the system architecture as this enables

the consolidation and sharing of IT resources through a single, easy-to-deploy management interface. Virtualised services operate and offer benefits at many levels—sharing servers or storage devices, supporting secure access to systems, enabling safe failover and restoring data to a trusted state. Virtualisation is the way to the next stage of consolidation.

## Education: Storage Security Standards What Are They and What Do They Mean to Storage Consumers?

Andrew Nielsen, CISSP, CISA, ISSAP, ISSMP; SNIA Security Technical Working Group



It has long been said that storage is one of the “last frontiers” to be exposed to security. Post 9/11, there has been a flurry of activity around securing information as it moves, rests, and is archived for the long term. Several varieties of security technologies have been thrown at this goal with limited market adoption though some of it continues to survive post acquisition and integration into core infrastructure products.

Accompanying the proliferation of technology has been a number of standards initiatives that are now driving security into the core functionality of the storage ecosystem. Since

these standards activities are in various phases of development and completion, they operate in largely isolated environments. In the interim, the storage user will struggle with the reality of the famous quote “That’s the nice thing about standards—there being so many to choose from.”

In order to make standards a bit more palatable, they can be grouped into the following courses or domains: storage management and services, fabric security, encryption in storage, and IP services retrofit.

The following table outlines the current domains and their relevant activities.

*(Continued on page 6)*

Domain	Standards Body	Standards Activity
Storage management and services	Storage Networking Industry Association	Storage Management Initiative Specification (SMI-S) eXtensible Access Method (XAM)
Fabric security	INCITS T10	SCSI Object-Based Storage Device Commands (OSD) SCSI Primary Command Set (SPC-4) SCSI Stream Commands (SSC-3)
	INCITS T11	Fibre Channel Security Protocol (FC-SP) Fibre Channel Security Protocol v2 (FC-SP-2)
Encryption In storage	IEEE P1619	IEEE P1619-2007 IEEE P1619.1 IEEE P1619.2 IEEE P1619.3
	Trusted Computing Group	TCG Storage Architecture Core Specification
IP services retrofit	Internet Engineering Task Force	Simple Network Management Protocol (SNMPv3) Syslog Internet Protocol Version 6 (IPv6) Transport Layer Security (TLS)

## Education: Storage Security Standards

(Continued from page 5)

This article summarises each of the domains. For the complete document, and more information on how each domain rolls up into a different industry or standards organisation, as well as what users can do as they wait for storage security standards to be approved and vendors to implement, visit the SNIA Storage Security Industry Forum website at [http://www.snia.org/forums/ssif/knowledge\\_center/articles/](http://www.snia.org/forums/ssif/knowledge_center/articles/)

## Storage Management and Services

In the domain of storage management and services, SNIA is actively developing open standards for uniform storage management and services as part of its mission is to lead the storage industry worldwide in developing and promoting standards, technologies, and educational services to empower organisations in the management of information. Two of the association's key standards initiatives with relevance to storage security are the Storage Management Initiative Specification (SMI-S) and eXtensible Access Method (XAM). SMI-S defines a method for the interoperable management of a multi-vendor Storage Area Network (SAN). SMI-S version 1.1.1, which is almost an approved ANSI standard, employs a multi-level model, with specific Security Management Aspects regarding device-level security via basic authentication capabilities, connectivity-level security via basic device authentication, and access control management to storage volumes in the fabric.

Transitioning from managing storage to accessing archived information, the XAM (eXtensible Access Method) Interface specification defines a standard access method to support ILM-based practices, long term records retention, and information security. Via the XAM Application Programming Interface (API), the specifications seek to manage the relationship between applications, management software and storage systems to manage fixed content reference information storage services. XAM includes specific metadata definitions to accompany data XAM, whose version 1 architecture specification is still under development.

## Fabric Security

While SNIA owns the standards around storage management and access methods, the International Committee for Information Technology Standards (INCITS) is where the action is when it comes to SCSI and Fibre Channel (FC) security. Under the purview of INCITS, sit two committees that are squarely in charge of SCSI and Fibre Channel Security: T10 and T11.

## INCITS Technical Committee T10

INCITS T10's principal work is the Small Computer System Interface (SCSI), including a variety of architecture, command set standards that are all modern I/O interfaces, including SCSI, SAS, Fibre Channel, SSA, IEEE 1394, USB, and ATAPI (ATA).

On the most recently approved list of SCSI standards with security implication is the *SCSI Object-Based Storage Device Commands (OSD)*. The standard defines the command set extensions to control operation of Object-Based Storage devices. The objective of the standard is to permit an application client to communicate with a logical unit that declares itself to be a Object-Based Storage device; enable construction of a shared storage processor cluster with equipment and software from many different vendors; define commands unique to the type of SCSI Object-Based Storage devices; and define commands to manage the operation of SCSI Object-Based Storage devices. The standard defines the concept of a security manager, and credentials that enable the execution of specific commands on Object-based Storage class devices.

Currently under development in T10 are two efforts that seek to integrate security into the SCSI Primary Command Set (SPC-4), as well as SCSI Stream Commands (SSC-3).

SPC-4 defines a security model, and two commands named Security Protocol In & Security Protocol Out that enable a number of security protocols to be transported by a SCSI infrastructure. The Trusted Computing Group is one of the organizations taking advantage of this facility to create security protocols specifically for use by storage devices.

SSC-3 includes in the command set extensions new mode pages and protocols specifically created to support an encryption/decryption features contained within sequential-access devices. The protocols make use of the Security Protocol In & Security Protocol Out commands defined by the SPC-4 project.

## INCITS Technical Committee T11

INCITS T11's principal work is Fibre Channel (FC) including interface, protocol, switch and service definitions. This includes a variety of standards for FC physical and signalling, FC interconnection scheme standards, FC Generic Services Standards, and the FC Security Protocol standards.

(Continued on page 7)

## Education: Storage Security Standards

(Continued from page 6)

Published in December 2006, T10 is responsible for the creation of the Fibre Channel Security Protocol (FC-SP). The FC-SP project developed a set of methods that allow security techniques to be implemented in a Fibre Channel fabric. FC-SP includes Security Association (SA), Fabric Policy, and authentication services. These protocols provide means to guard against malicious attacks, accidental configuration changes, and to ensure tighter control of the deployment of fabric devices.

Following on the success of FC-SP, INCITS Project 1835 seeks to enhance Fibre Channel security in the form of FC-SP-2. Today, commonly deployed security techniques are centred about zoning and FC-SP techniques. FC-SP-2 will develop a set of additional and enhanced security services for the Fibre Channel fabric. Specifically this project will address Fabric Loop Security Issues, Authentication Material Distribution and Management, Fabric Credential Definition and Management, Security Associations Policy Management Interfaces, FC-IFR Security support, and SHA-256 support.

## Encryption in Storage

As we move through the storage ecosystem from protecting data in the fabric to securing data on disk, there are many activities underway in various states of approval and development. Activities around security data at rest are largely driven by two entities: IEEE 1619 and the Trusted Computing Group (TCG).

### Institute of Electrical and Electronics Engineers (IEEE) 1619

IEEE 1619, which is also referred to as the Security In Storage Working Group (SISWG), is charged with developing standards for the protection of information on storage media. In this working group, there are four standards with status ranging from "approved" to "still under development."

The first approved standard from IEEE 1619 is the *Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices (IEEE 1619-2007)*. 1619-2007's primary purpose is to describe encryption methods for data stored in sector-based devices as well as specifying encryption methods and import/export methods of encryption keys for interoperability between different implementations. The 1619-2007 standard also specifies the use of a tweakable block cipher (XTS-AES) and its use in sector-based storage. XTS-AES addresses a variety of threats, while allowing parallelization and pipelining of cipher implementations.

Another 1619 activity that is in an approved state is the *Standard for Authenticated Encryption with Length Expansion for Storage Devices (1619.1)*. 1619.1, which should be published in the very near future, seeks to provide methods for ensuring the privacy and integrity of stored data within high-assurance applications. Similar to IEEE 1619-2007, IEEE 1619.1 also prescribes the use of AES encryption using authenticated encryption modes (GCM and CCM) that allow for authentication and length expansion. While the standard is valuable to vendors in the creation and development of cryptographic modules, its true value is to the consumer. This standard really affords the consumer of encryption technology a measuring stick by which to evaluate the quality of cryptographic devices based on compliance with 1619.1.

Exploring the "under development" realm of IEEE 1619, there are two activities that round out protection of data on disk. Those two activities are the *Standard for Wide-Block Encryption for Shared Media (IEEE P1619.2)* and the *Standard for Key Management Infrastructure for Cryptographic Protection of Stored Data (IEEE P1619.3)*.

1619.2 is an architecture specification for media security where an attacker has repeated access to encrypted data both in-flight and at rest. While 1619.2 is really geared to dealing with fixed-size encryption blocks, it is anticipated that future development of the standard will allow for data expansion, which will help prevent against data tampering.

While encryption of data on paper looks great, the market has been slow to adopt large scale encryption strategies as there has never been a uniform way to manage encryption keys that allows for vendor independence. IEEE 1619.3 seeks to address key management issues by specifying architecture for the infrastructure required to manage cryptographic protections for stored media. Additionally, this activity also manages the protections defined in the other 1619 standards.

### Trusted Computing Group

Moving away from IEEE, the Trusted Computing Group (TCG) is also working on defining security protections for sector-based devices. The TCG seeks to develop, define, and promote open standards for hardware-enabled trusted computing and security technologies, with their primary goal being to help users protect their information assets from compromise due to external software attack and physical theft.

(Continued on page 8)

## Education: Storage Security Standards

(Continued from page 7)

The first version of the *TCG Storage Architecture Core Specification* is still currently under development. This TCG specification seeks to provide an architecture for applying policy-based access control to select storage features. This policy based control would allow storage devices to participate as part of a trusted platform. While the intended audience of the specification is storage device and peripheral device manufacturers, it is also useful for developers that may wish to integrate storage devices and peripherals into trusted platforms.

### IP Services Retrofit (Courtesy of the IETF)

In recent history the storage and networking worlds collided. With the advent of connected infrastructures, IT compliance, executive dashboards, and single-pane of glass management interfaces, the storage world has been forced to integrate with a variety of internetwork services and protocols of varying security postures. Most of these protocols and services, from a standards perspective, are managed by the Internet Engineering Task Force (IETF).

The IETF formally under the purview of the Internet Society, develops and promotes Internet standards, cooperating closely with the W3C and ISO/IEC standard bodies; and dealing in particular with standards of the TCP/IP and Internet protocol suite. Based on the broad scope of the work in the IETF, some of most relevant activity to storage security is SNMPv3, Syslog, IPv6, and TLS.

### SNMPv3

The Simple Network Management Protocol (SNMP) is arguably the most commonly utilized network management Protocol (SNMP) on IP-based networks. The IETF recognizes SNMPv3 as defined by RFC 3411–RFC 3418 as the current standard version of SNMP as of 2004. Previous versions of SNMP lacked any security features mostly in the areas of authentication and confidentiality. SNMPv3 provides secure access to network based devices (including storage devices) using Message integrity, Authentication, and Encryption. As many network centric vendors have embraced SNMPv3, so are various storage vendors as this functionality is starting to appear in a variety of product offerings.

### Syslog

While SNMP is the common for network management, Syslog is by far the most commonly utilized protocol for event logging of network based devices even though it was never a formal IETF standard. In the last few years, Syslog

has become a standard feature on a variety of storage products as compliance and regulatory requirements continue to demand traceability of administrative actions. While many of the major storage vendors support the use of Syslog, the protocol has had its security challenges

The Syslog Working Group under the purview of the IETF is charged with standardizing the Syslog protocol and its transport mechanism (currently UDP-based), and remediate the security issues around modification, disclosure, and masquerading. Based on this charter the Syslog Working Group has produced multiple draft standards to address these issues. The relevant draft standards for Syslog are:

- *Syslog Management Information Base (draft-ietf-syslog-device-mib-17)*
- *The Syslog Protocol (draft-ietf-syslog-protocol-23)*
- *Transmission of Syslog messages over UDP (draft-ietf-syslog-transport-udp-12)*
- *TLS Transport Mapping for Syslog (draft-ietf-syslog-transport-tls-11)*

### Internet Protocol v6

While it is well known that IPv6 was generally put in place to deal with IPv4 address exhaustion it also came with built-in transports security in the form of IPSec. The core IPv6 standards are widely implemented and are starting to see global deployment. While the IETF Editor has published three RFCs for IPv6 (RFC 4294, 4291, and 2460), even the US Federal Government has gotten in on the action publishing its own draft guidance in the form of NIST 500-267, which specifies the use of IPSec and cites specific cipher suites that must be supported.

As far as relevance to storage, there has been much discussion in the last year around the lack of security associated with various storage protocols such as CIFS, NFSv3, iSCSI, and iSNS. With customers slow to demand and deploy updated versions of these protocols, IPv6 with its native transport security in the form of IPSec may breathe new life into aging access methods.

### Transport Layer Security (TLS)

The TLS protocol allows applications to communicate across a network in order to prevent eavesdropping, tampering, and message forgery. TLS is specified for transport security in SMI-S, Syslog, SNMP, and IEEE 1619 activities.

(Continued on page 9)

## Education: Storage Security Standards

(Continued from page 8)

Established in 1996 The TLS Working Group was charged with standardizing a transport layer security protocol. Starting with SSL version 3.0, the working group has completed a series of specifications that describe the Transport Layer Security (TLS) protocol versions 1.0 (RFC 2246) and 1.1 (RFC 4346), extensions to the protocol, and new cipher suites to be used with TLS. Future work will include publishing a revision of TLS, version 1.2 (*draft-ietf-tls-rfc4346-bis-10*) that removes the protocol's dependency on the MD5 and SHA-1 digest algorithms. Version 1.2 will also provide new authenticated encryption modes and cipher suites for TLS.

## Conclusions

While storage may be the next frontier for the integration of security, there is definitely no lack of activity to define standards in this space. While it is clear that all the major parts of the storage ecosystem have some amount of security activities underway or recently approved, what is not clear is how well all these standards will converge in the larger sandbox of the storage infrastructure as deployed by storage

users. Lack of integration at the standards can lead to customer confusion, slow adoption rates, and vendors devising proprietary implementations as they push to get products to market to address end user needs. Such proprietary solutions limit customer flexibility and promote technology dependence, which can ultimately limit business agility.

Other than a few limited examples, most of these activities operate in fairly isolated environments with limited or non-existent communication between them. Most of the cross-talk between these security activities takes place in the SNIA Security Technical Working Group (SSIF TWG) and the SNIA Storage Security Industry Forum (SSIF). Going forward, SNIA will continue to be the nexus for monitoring these standards. For more information about the SSIF – visit [www.snia.org/ssif](http://www.snia.org/ssif).

## Regional Committee Update: France

Philippe Nicolas, Director and French Committee Chair, SNIA Europe, [francechair@snia.org](mailto:francechair@snia.org)



The SNIA Europe French Committee has been rather busy in the past few months. Just a few weeks ago, we held the latest round of elections and welcomed industry experts Philippe Reynier (Bull) to the position of Technical Committee Chair, and Laurent Bartoletti (SUN) and Philippe Nicolas (Brocade) to the positions of

Vice Chair and Chair respectively. In addition, the committee welcomes its three newest member companies: Active Circle, Atempo and Bull.

The newly elected leadership team are already working to develop a compelling program for the next SNIA Europe Academy in Paris on 17<sup>th</sup> March 2009.

In France, a mature market in terms of technology adoption, we are seeing the same unstoppable evolution of the data centre towards maximum efficiency, performance and security as is being experienced in many other countries.

Among the most interesting technologies, some of them already available on the market, are data de-duplication, security through encryption, virtualisation, thin provisioning associated with advanced file storage (particularly parallel storage), Ethernet (e.g. FCoE), cloud computing/storage, and of course the development of the “green” practices. The SNIA Europe Academy in Paris will be the perfect opportunity to meet with industry experts to discuss these and other hot topics such as storage resource optimisation, data de-duplication, and long-term data retention and preservation with references to XAM (eXtensible Access Method).

**Mark your diaries now** for the SNIA Europe Academy in Paris, 17 March 2009. Go to [www.storage-academy.com](http://www.storage-academy.com) for further information and to secure your place.

**Industry Events 2008****October 27-29**

SNW Europe  
Frankfurt

**November 5-9**

IDC IT Security, Storage & Business  
Continuity Roadshow 2008  
Multiple Cities: Riyadh, Dubai

**November 10-13**

SNIA Technical Symposium  
San Diego

**November 12-13**

Storage Expo Netherlands  
Utrecht

**November 18**

Storage Virtualization  
London

**November 19**

Storage, Backup & Recovery 08  
Zurich

**November 19-December 3**

Middle East and Africa Virtualization  
and Green Datacenters 2008  
Multiple Cities:  
Johannesburg, Doha, Casablanca

**November 20**

Green IT Conference 2008  
Amsterdam

**November 27**

BITKOM Anwenderforum IT-Infrastruktur  
Frankfurt

**Industry Events 2009****January 20-23**

SNIA Winter Symposium  
San Jose

**January 27**

SNIA Europe Academy  
Zurich

**February 3**

SNIA Europe Academy  
Dubai

**February 24-25**

Data Centre World  
Conference & Expo  
London

**March 16-20**

SNIA Technical Symposium  
San Jose

**March 17**

SNIA Europe Academy  
Paris

**March 24**

SNIA Europe Academy  
Stockholm

**March 26**

SNIA Europe Academy  
Copenhagen

**April 6-9**

SNW USA  
Orlando

**May 19**

SNIA Europe Academy  
London

**Full Event**

**Calendar with weblink on:**  
<http://www.snia-europe.org>



**STORAGE NETWORKING  
INDUSTRY ASSOCIATION EUROPE**

Erico House, Suite 406  
93-99 Upper Richmond Road  
London SW15 2TG  
United Kingdom

Phone: + 44 (0) 20 8785 5555  
Fax: + 44 (0) 20 8785 5624  
Email: [euroinfo@snia.org](mailto:euroinfo@snia.org)  
Web: <http://www.snia-europe.org>

**Subscribe to Storage Networking Times**

[www.snia-europe.org/subscribe](http://www.snia-europe.org/subscribe)